UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/462,616	04/03/2000	GUNTER MARINGER	0745/61002/N	5313

7590 04/21/2006

NORMAN H ZIVIN
COOPER & DUNHAM
1185 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/462,616	MARINGER ET AL.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *16-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 01/26/06. The amendment filed on 01/26/06 have been entered and made of record. Therefore, presently pending claims are 16-39.

Response to Arguments

Applicant's arguments filed 01/26/06 have been fully considered but they are not persuasive because of following reasons.

Applicant argued, "...applicants are uncertain whether this document was ever published and therefor, whether it constitutes prior art..." This is not found persuasive since the document itself recites "... SRC Research Report 39 was originally published on February 28, 1989..." The paper is also freely available on the Internet.

Applicant argued that Burrows fails to transmit N_A that is assumed to correspond with Response 2. In so doing, the applicant has requested the examiner to provide a reference for the common knowledge rejection. The reference, indicating nonce values sent between devices for Mutual authentication, is provided below.

The applicant argued further that Burrow does not teach Response 1 = Challenge 2. This is not found persuasive. The claims 16 and 28 do not claim Response 1 = Challenge 2. The claims recites "...wherein the network is authenticated by the terminal by matching a second calculated response, calculated by the terminal based on the first random number (challenge 1) with the second response (response 2)..." The term "match" may mean equal, however, it also means a pair suitably associated. Therefore the terms $\{N_B - 1\}$ K_{AB} and the nonce N_A are a

matching pair suitably associated because the nonce N_A is used to authenticate the key K_{AB} therefore the pair cannot be utilized one without the other and are therefore suitably associated. It follows that the reference Burrows does teach "...matching a second calculated response, calculated by the terminal based on the first random number (challenge 1) with the second response (response 2)..."

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 16-18, 20, 25-30, and 37-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over the article by Burrows ("A Logic of Authentication") in view of the article by Shieh et al ("An Efficient Authentication Protocol for Mobile Network").

In reference to claims 16 and 28 Burrows discloses the Needham-Schroeder in which A and B are mutually authenticated (Section 5 pages 17-18). The authentication system of Needham-Schroeder includes the steps listed below. Receiving, at the network, a triplet data set from an authentication center, the triplet data set including a first random number (challenge 1), a first response (response 1) and a second response (response 2) {page 18 message 2}, wherein Na corresponds to the second response; Kab corresponds to the first response; and Kab encrypted by Kbs, (Kab, A)Kbs, corresponds to the first challenge. Sending the first random number (challenge 1) to the terminal; wherein the first random number corresponds to the encrypted

value (Kab, A) encrypted by Kbs, and B corresponds to the terminal (page 18). Receiving, from the terminal, a first calculated response, calculated by the terminal based on the first random number (challenge 1), wherein the first calculated response is used as a second challenge (challenge 2) {page 18}. A sends the message 3 which is the first challenge that is followed by a response by B wherein B calculates the decryption of the key Kab and sends the response {Nb}Kab and first response. In the system disclosed by Burrow A authenticates the terminal, B, by matching the first calculated response with the first response that corresponds with message 4. The system then sends the message 5 that corresponds to the second response to the terminal. The network is authenticated by the terminal by matching a Nonce (Nb), which performs the function of the second response, and the calculated response using the message 4, which corresponds to the first response with the response calculated by the terminal form the first random number with the second response.

As stated earlier, the nonce Na corresponds to the second response, however this particular nonce is not sent from A to B as the second response.

Shieh discloses a mutual authentication system wherein the nonce is sent from the user to the server and the server from the user. The nonce is used to prove the freshness of the session key (section 2.1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the Nonce that is sent from server S as the nonce that is sent to the terminal B for the mutual authentication process and therefore perform the function of the second response as taught by Shieh in the system of Burrows. One of ordinary skill in the art would have been motivated to do this because the system already sends a nonce from the server S and

the system A is able to decrypt the data sent from the server S and then forward the information to B, further using the nonce that is sent from the server S would reduce the amount of processing that the terminal B would be required to perform and therefore decrease the processing time.

In reference to claims 17 and 29 the terminal calculates the response from the first random number using an internally stored key {Kbs, page 18}.

In reference to claims 18 and 30 the terminal calculates the second calculated response form the first random number {message 3}.

In reference to claim 20 wherein to use the first calculated response of the terminal as the second challenge (Challenge 2), a shorter length of the first calculated response is filled out make up a greater length of the second challenge (Challenge 2) {message 3 page 18}.

In reference to claims 27 and 38-39 wherein the authentication center calculates the triplet data sets requested by the network and transmits the calculated triplet data set to the network off-line and independently of time, on request by the network, and before data interchange between the network and the terminal {page 18}.

In reference to claims 25-26 and 37, wherein the network is a wire-based network (see Fig. on page 18).

Claims 19 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burrow as applied to claim 16 above, and further in view of Douceur et al (6,021,203).

Wherein multiple triplet data sets are received from the authentication center and stored on the network as a stockpile to reduce the number of times triplet data sets must be received.

Although Burrows discloses sending the triplet from the authentication center, S, to the A, Burrow does not expressly disclose sending multiple triplet data sets as a stockpile.

Douceur discloses a protocol provided for transmitting low security messages and high security messages with one-time pad cryptosystem (abstract). The system sends multiple keys that correspond to the multiple triplets (part 46 Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to sending multiple triplet data sets as a stockpile as in Douceur in the key exchange between the server and A in the system of Burrows. One of ordinary skill in the art would have been motivated to do this because the use of large non-repeating set of truly random key letters creates a high security encryption method.

Claims 21-24, 32-35, 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burrow as applied to claim 16 above, and further in view of Tsubakiyama (5,544,245)

In reference to claim 24 and 36, wherein the network is a GSM network and wherein the network is a wire-based network. Tsubakiyama discloses the network in Fig. 2. The GSM is a type of wireless network and therefore is encompassed in Tsubakiyama's description.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to method of Tsubakiyama. One of ordinary skill in the art would have been motivated to do this because wireless devices are more portable therefore a system with wireless connection provides the user flexibility.

In reference to claims 21, 32, and 35 wherein the filling-out is performed on a subscriber-specific basis; and the complete length of the first calculated response is shortened before transmission.

Tsubakiyama discloses the manipulation of the data sent to the subscriber (user) to create a key (column 5 lines 12-15).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to the filling-out is performed on a subscriber-specific basis; and the complete length of the first calculated response is shortened before transmission. One of ordinary skill in the art would have been motivated to do this because it would tailor the system to the users needs and therefore make the system more flexible.

In reference to claim 22-23 and 33-34 wherein the first calculated response is filled out with defined bits from an internally stored key to make up the length of the second challenge.

Tsubakiyama discloses the manipulation of the data sent to the subscriber (user) to create a key (column 5 lines 12-15).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to fill out the first calculated response with defined bits form an internally stored key to make up the length of the second challenge. One of ordinary skill in the art would have been motivated to do this because longer keys are safer keys and therefore the lengthening of the keys will increase the security of the system.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Tuesday, April 11, 2006

HOSUK SONG
PRIMARY EXAMINER